Federal Family Education Loan System (FFELS)
Corrective Action Plan,
September 2000

No	Control Area	Observation	Concur with Observation	Corrective Action / Description	Completion Date	Point of Contact
1	Security Life Cycle Planning	There was no evidence of appropriate security controls for each phase of the System Development Life Cycle.		Ensure that (as appropriate) privacy and security in the information life cycle are addressed in FFEL life cycle planning documents. See the Security Life Cycle Planning section for additional details		
2	Rules of Behavior	There was no evidence that the Rules of Behavior were documented.		Document rules of behavior for FFEL. Ensure managers and users are trained to understand them.		
3	Authorize Processing	Although FFEL has not sought certification, this report could serve as the basis for a system certification/ authority to operate.		Obtain an IATO for one year from the OCIO as soon as practical. Within eighteen months from issuance of the IATO, perform a formal FFEL certification test under NIST guidance (FIPS 102).		
4	Application Software Maintenance Controls	Application development/testing processes needed to be reviewed. SSO role had not been formalized in the Configuration Management (CM) process.		Examine ED guidance relating to system life cycle planning. Ensure FFEL CM processes and procedures are consistent with that guidance, and that the FFEL SSO is integrated into the systems development and CM processes. SSO should be part of the approval chain for all proposed changes to system software.		
5	Personnel Security	Security clearance processing management needed improvement. Uniform and consistent personnel security policies should be implemented at all E-Systems locations associated with FFEL.		Implement ED personnel security guidance. See the Personnel Security section for additional details.		

No	Control Area	Observation	Concur with Observation	Corrective Action / Description	Completion Date	Point of Contact
6	Security Awareness and Training	Security awareness training needed to be improved for ED staff, and in-depth training needed to be provided to additional personnel.		Provide security training for the FFEL SSO; once trained, the FFEL SSO should assist the OCIO in setting up an entity-wide security awareness and training program. See the Security Awareness and Recommendations sections for detailed guidance.		
7	Logical Access Controls	Documented most recently in the FFEL Sensitive Application Certification Review Report, July 1996. Ensure that individual accountability is established and maintained for the LAN development activities.		Document and implement within one year FFEL-specific policies, standards, procedures and guidelines to govern logical access processes and mechanisms.		
8	Contingency Planning	Develop a Disaster Recovery Plan (DRP) and Continuity of Operations Plan for the Ballston facility. Disaster Recovery Plan (DRP) has not been kept current.		Ensure formal contingency and incident response plans are consistent with NIST guidance (Special Pub 800-3). Ensure plans are exercised once annually, and the FFEL SSO has a copy of all plans.		
9	Documentation	Security Plan needed to be updated based upon a recent revision of OMB Circular A-130.		Develop a NIST-compliant (Special Pub 800-18) security plan for FFEL. See the Recommendations section for additional details.		
10	Identification and Authentication	There was no evidence that password usage was being managed/monitored.		Ensure FFEL complies with SFA standards for data user IDs and passwords. See the Identification and Authentication section above for detailed guidance.		
11	Audit Trails	There was no evidence to indicate the audit trails were being reviewed by appropriate staff.		Ensure FFEL audit results are being used effectively to help FFEL managers make appropriate risk decisions. See the Audit Trails and Recommendations sections for additional details.		
12	Data Integrity / Validation Controls	There was no evidence of controls for assuring the integrity and validity of the data.		Ensure FFEL complies with SFA standards for data integrity and automated validations. See the Data Integrity section for additional details.		

No	Control Area	Observation	Concur with Observation	Corrective Action / Description	Completion Date	Point of Contact
13	System Interconnection/ Information Sharing	There was no evidence of Memoranda of Understanding (MOU), or Trading Partner Agreements (TPA), or that the interfaces had been addressed in the Security Plan.		Ensure all FFEL connections and information sharing with non-SFA entities are codified. See the section above on system interconnection and information sharing for further details.		
14	Central Security Focus/ Assigned Responsibility			Ensure the CBS SSO is properly trained and qualified. See the section on security training and awareness, and the related recommendations for the Promote Awareness phase of the risk management cycle. In addition, a long-term computer security strategy, a compliance program, and descriptions of any liaison function for either external or intraorganizational entities should be documented.		
15	Public Access Controls	There was no evidence documenting whether or not public access was allowed to FFEL.		Document and implement within one year FFEL-specific policies, standards, procedures and guidelines to govern public access processes and mechanisms.		
16	Physical and Environmental Protection	Security enhancements were needed (e.g., require employees to display identification, provide safety training, secure items of value in locking cabinets, etc.).		When developing/updating the FFEL security plan, ensure the controls noted above are fully addressed.		
17	System Environment	There was no evidence of a technical description of the system.		See the recommendation for General Description/ Purpose above.		

No	Control Area	Observation	Concur with Observation	Corrective Action / Description	Completion Date	Point of Contact
18	Applicable Laws and Regulations	FFEL is cognizant of applicable laws and regulations. The status of Privacy Act compliance is unknown. Although this system presumably complies with notice, publication, and annual/biennial/quadrennial review requirements, as those remain the responsibility of the Department's Chief Privacy Officer, no system-specific information with regard to access controls, storage, retrieval, retention, disclosure logging, contractor compliance, disposal of records, or employee training was provided for these systems.		N/A		